Terms used **weak key cryptanalysis**

Found **134** of **203,282**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 134

Result page: **1** 2 3 4 5 6 7 next

Relevance scale □ ▭ ▬ ▬ ■

1 Survey and benchmark of block ciphers for wireless sensor networks ■

Yee Wei Law, Jeroen Doumen, Pieter Hartel

February 2006 **ACM Transactions on Sensor Networks (TOSN)**, Volume 2 Issue 1

Publisher: ACM Press

Full text available: pdf(354.39 KB)

Additional Information: full citation, appendices and supplements, abstract, references, index terms

Cryptographic algorithms play an important role in the security architecture of wireless sensor networks (WSNs). Choosing the most storage- and energy-efficient block cipher is essential, due to the facts that these networks are meant to operate without human intervention for a long period of time with little energy supply, and that available storage is scarce on these sensor nodes. However, to our knowledge, no systematic work has been done in this area so far. We construct an evaluation framew ...

Keywords: Sensor networks, block ciphers, cryptography, energy efficiency

2 High speed networking security: design and implementation of two new DDP-based ciphers ▬

N. Sklavos, N. A. Moldovyan, O. Koufopavlou

February 2005 **Mobile Networks and Applications**, Volume 10 Issue 1-2

Publisher: Kluwer Academic Publishers

Full text available: pdf(643.16 KB)

Additional Information: full citation, abstract, references, index terms, review

Using Data-Dependent (DD) Permutations (DDP) as main cryptographic primitive two new ciphers are presented: ten-round Cobra-H64, and twelve-round Cobra-H128. The designed ciphers operate efficiently with different plaintext lengths, 64 and 128-bit, for Cobra-H64 and Cobra-H128, respectively. Both of them use very simple key scheduling that defines high performance, especially in the case of frequent key refreshing. A novel feature of Cobra-H64 and Cobra-H128 is the use of the Switchable Operatio ...

Keywords: Cobra-H128, Cobra-H64, data-dependent permutations, encryption, networking security

3 Computer security (SEC): Efficient Diffie-Hellmann two-party key agreement protocols based on elliptic curves ▬

Maurizio Adriano Strangio
March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '05**
Publisher: ACM Press
Full text available: pdf(234.27 KB) Additional Information: full citation, abstract, references, index terms

Key agreement protocols are of fundamental importance for ensuring the confidentiality of communications between two (or more) parties over an insecure network. In this paper we review existing two-party protocols whose security rests upon the intractability of Diffie-Hellmann and Discrete Logarithm problems over elliptic curve groups. In addition, we propose a new two-party mutual authenticated key agreement protocol and collectively evaluate the security and performance of all the schemes cons ...

Keywords: cryptography, elliptic curves, key agreement, protocols

4 The design of substitution-permutation networks resistant to differential and linear cryptanalysis
H. M. Heys, S. E. Tavares
November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security CCS '94**
Publisher: ACM Press
Full text available: pdf(748.62 KB) Additional Information: full citation, abstract, references, index terms

In this paper we examine a class of product ciphers referred to as substitution-permutation networks. We investigate the resistance of these cryptographic networks to two important attacks: differential cryptanalysis and linear cryptanalysis. In particular, we develop upper bounds on the differential characteristic probability and on the probability of a linear approximation as a function of the number of rounds of substitutions. Further, it is shown that using large S-boxes with good diffu ...

5 Ganzúa: A cryptanalysis tool for monoalphabetic and polyalphabetic ciphers
Jesús Adolfo García-Pasquel, José Galaviz
September 2006 **Journal on Educational Resources in Computing (JERIC)**, Volume 6 Issue 3
Publisher: ACM Press
Full text available: pdf(4.18 MB) Additional Information: full citation, abstract, references, index terms

Many introductory courses to cryptology and computer security start with or include a discussion of classical ciphers that usually contemplates some cryptanalysis techniques used to break them. Ganzúa (picklock in Spanish) is an application designed to assist the cryptanalysis of ciphertext obtained with monoalphabetic or polyalphabetic ciphers. It can use almost arbitrary character sets for the plain and cipher alphabets as well as obtain the standard relative frequencies of many lang ...

Keywords: Cryptology, classical cryptography

6 An experiment on DES statistical cryptanalysis
Serge Vaudenay
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security CCS '96**
Publisher: ACM Press
Full text available: pdf(786.82 KB) Additional Information: full citation, references, citings, index terms

7 An introduction to side channel cryptanalysis of RSA

Artemios G. Voyiatzis
May 2005 **Crossroads**, Volume 11 Issue 3
Publisher: ACM Press
Full text available: html(18.63 KB) Additional Information: full citation, references, index terms

8 Differential cryptanalysis of hash functions based on block ciphers □
Bart Preneel, Rene Govaerts, Joos Vandewalle
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press
Full text available: pdf(609.16 KB) Additional Information: full citation, abstract, references, index terms

This paper describes a differential attack on several hash functions based on a block cipher. The emphasis will be on the results for cases where DES [8] is the underlying block cipher. It will briefly discuss the case of FEAL-N [19, 21].

9 Cryptosystem and analysis: Cryptanalysis of the "Grain" family of stream ciphers □
Alexander Maximov
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(234.26 KB) Additional Information: full citation, abstract, references, index terms

Let us have an NLFSR with the feedback function *g(x)* and an LFSR with the generating polynomial *f(x)*. The function *g(x)* is a Boolean function on the state of the NLFSR and the LFSR, at any time instance *t*. Whenever the LFSR has good statistical properties, it is used for controlling the randomness of the NLFSR's state machine. In this paper we define and study the general class of "Grain" family of stream ciphers, where the keystream bits are generated by another Bool ...

Keywords: correlation attacks, cryptanalysis, decoding problem, distinguisher, grain

10 Cryptanalysis of some encryption/cipher schemes using related key attack □
NOTE FROM ACM: It has been determined that the authors of this article plagiarized the contents from a previously published paper. Therefore ACM has shut off access to this paper.
Khawaja Amer Hayat, Umar Waqar Anis, S. Tauseef-ur-Rehman
June 2004 **ACM SIGCSE Bulletin , Working group reports from ITiCSE on Innovation and technology in computer science education ITiCSE-WGR '04**, Volume 36 Issue 4
Publisher: ACM Press
Additional Information: full citation, abstract, references

NOTE FROM ACM: It has been determined that the authors of this article plagiarized the contents from a previously published paper. Therefore ACM has shut off access to this paper.

To see the paper that was plagiarized, click here

Additional Links

The citation in ACM's Guide to Computing Literature, ...

Keywords: DES, cryptanalysis, differential related key attacks, related key attack

11 Cryptanalysis and protocol failures (abstract) □

Gustavus J. Simmons

December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**

Publisher: ACM Press

Full text available: pdf(164.92 KB) Additional Information: full citation, abstract, index terms

In this lecture examples will be given of key distribution protocols that distribute keys to unintended recipients, secrecy protocols that publicly reveal the contents of (supposedly) secret communications, digital signature protocols that make forgery easy — all based on cryptoalgorithms that are sound so far as is known. In at least one case the cryptographic algorithm that is employed is Vernam encryption/decryption with a properly chosen one time key which is well known to be unco ...

12 Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers □

Ramesh Karri, Kaijie Wu, Piyush Mishra, Yongkook Kim

June 2001 **Proceedings of the 38th conference on Design automation DAC '01**

Publisher: ACM Press

Full text available: pdf(260.32 KB) Additional Information: full citation, abstract, references, index terms

Fault-based side channel cryptanalysis is very effective against symmetric and asymmetric encryption algorithms. Although straightforward hardware and time redundancy based concurrent error detection (CED) architectures can be used to thwart such attacks, they entail significant overhead (either area or performance). In this paper we investigate systematic approaches to low-cost, low-latency CED for symmetric encryption algorithms based on the inverse relationship that exists between encryp ...

13 Book reviews: Comparative book review: Cryptography: An Introduction by V. V. Yaschenko (American Mathematical Society, 2002); Cryptanalysis of Number Theoretic Ciphers by S.S. Wagstaff, Jr. (Chapman & Hall/CRC Press, 2003); RSA and Public-Key Cryptography by R. A. Mollin (Chapman & Hall/CRC Press, 2003); Foundations of Cryptography, vol. 1: Basic Tools by O. Goldreich, (Cambridge University Press, 2001) □

Jonathan Katz

June 2005 **ACM SIGACT News**, Volume 36 Issue 2

Publisher: ACM Press

Full text available: pdf(2.79 MB) Additional Information: full citation, abstract, index terms

With the growing interest in cryptography --- from students and researchers as well as from the general public --- there has been a corresponding increase in the number of cryptography textbooks available. Many of these, however, remain somewhat mired in the past, and present cryptography from a pre-1980s point of view. Indeed, there are very few published books which even make an attempt (let alone a successful one) at covering *modern* cryptography. This unfortunate state of af ...

14 Cryptanalysis of a flexible remote user authentication scheme using smart cards □

Wei-Chi Ku, Shuai-Min Chen

January 2005 **ACM SIGOPS Operating Systems Review**, Volume 39 Issue 1

Publisher: ACM Press

Full text available: pdf(406.12 KB) Additional Information: full citation, abstract, references, index terms

In 2002, Lee, Hwang, and Yang proposed a verifier-free remote user authentication scheme using smart cards. Their scheme is efficient because of mainly using cryptographic hash functions. However, we find that Lee-Hwang-Yang's scheme is not reparable once the user's permanent secret is compromised and is vulnerable to a privileged insider's attack. Furthermore, it lacks the user eviction mechanism. In this paper, we first show the weaknesses of Lee-Hwang-Yang's scheme, and then compare Lee-Hwang ...

Keywords: authentication, password, privileged insider's attack, reparability, user eviction

15 Systematic generation of cryptographically robust S-boxes □
Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press
Full text available: pdf(1.20 MB) Additional Information: full citation, abstract, references, index terms

Substitution boxes (S-boxes) are a crucial component of DES-like block ciphers. This research addresses problems with previous approaches towards constructing S-boxes, and proposes a new definition for the robustness of S-boxes to differential cryptanalysis, which is the most powerful cryptanalytic attack known to date. A novel method based on group Hadamard matrices is developed to systematically generate S-boxes that satisfy a number of critical cryptographic properties. Among the propert ...

16 Battery power-aware encryption □
R. Chandramouli, S. Bapatla, K. P. Subbalakshmi, R. N. Uma
May 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 2
Publisher: ACM Press
Full text available: pdf(454.71 KB) Additional Information: full citation, abstract, references, index terms

Minimizing power consumption is crucial in battery power-limited secure wireless mobile networks. In this paper, we (a) introduce a hardware/software set-up to measure the battery power consumption of encryption algorithms through real-life experimentation, (b) based on the profiled data, propose mathematical models to capture the relationships between power consumption and security, and (c) formulate and solve security maximization subject to power constraints. Numerical results are presented t ...

Keywords: Low-power encryption, optimization, profiling

17 Attacks and cryptanalysis: A natural language approach to automated cryptanalysis of two-time pads □
Joshua Mason, Kathryn Watkins, Jason Eisner, Adam Stubblefield
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(230.76 KB) Additional Information: full citation, abstract, references, index terms

While keystream reuse in stream ciphers and one-time pads has been a well known problem for several decades, the risk to real systems has been underappreciated. Previous techniques have relied on being able to accurately guess words and phrases that appear in one of the plaintext messages, making it far easier to claim that "an attacker would never be able to do *that*." In this paper, we show how an adversary can automatically recover messages encrypted under the same keystream if only the ...

Keywords: keystream reuse, one-time pad, stream cipher

18 Applied cryptography: Cryptanalysis of a provably secure CRT-RSA algorithm □
David Wagner
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**
Publisher: ACM Press
Full text available: pdf(131.85 KB) Additional Information: full citation, abstract, references, index terms

We study a countermeasure proposed to protect Chinese remainder theorem (CRT) computations for RSA against fault attacks. The scheme was claimed to be provably secure. However, we demonstrate that the proposal is in fact insecure: it can be broken with a simple and practical fault attack. We conclude that the proposed countermeasure is not safe for use in its present form.

Keywords: RSA, chinese remainder theorem, cryptanalysis, fault attacks

19 Technical opinion: designing cryptography for the new century □
Susan Landau
May 2000 **Communications of the ACM**, Volume 43 Issue 5
Publisher: ACM Press
Full text available: pdf(215.10 KB) html(35.06 KB) Additional Information: full citation, references, index terms

20 Cryptography and data security □
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, citings, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

Results 1 - 20 of 134 Result page: **1** 2 3 4 5 6 7 next

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L5	141	(380/2).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/06/13 21:22
L6	323	(726/25).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/06/13 21:44
L7	1	("20050180315").PN.	US-PGPUB; USPAT	OR	OFF	2007/06/13 21:44
L9	962	cryptanalysis	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 22:45
L10	206	cryptanalysis same weak same key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 22:45
S1	1	("20050157879").PN.	US-PGPUB; USPAT	OR	OFF	2007/06/12 20:36
S2	207	weak adj key with (detect$3 test$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:29
S3	3	(weak adj key with (detect$3 test$3)).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 20:36
S4	205	weak adj key with (detect$3 test$3) and (cipher encrypt scramble)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:14
S5	8	weak adj key with (detect$3 test$3) and (cipher encrypt scramble).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:08

EAST Search History

S6	155	weak adj key with (detect$3 test$3) same (encrypt$3 encipher$3 cryptograph$2 scrambl$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:14
S7	0	("2005/0157879").URPN.	USPAT	OR	ON	2007/06/12 21:13
S8	9	weak with key with (detect$3 test$3) same (encrypt$3 encipher$3 cryptograph$2 scrambl$3) not S6	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:14
S9	0	("2005/0235342").URPN.	USPAT	OR	ON	2007/06/12 21:17
S10	1	("6397330").PN.	US-PGPUB; USPAT	OR	OFF	2007/06/12 21:19
S11	2	(("7079648") or ("5963646")).PN.	US-PGPUB; USPAT	OR	OFF	2007/06/12 21:19
S12	2	("5689565" | "6397330").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/06/12 21:20
S13	4	("6397330").URPN.	USPAT	OR	ON	2007/06/12 21:26
S14	12	(weak with semi adj weak) same (encrypt$ cryptograph$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:42
S15	1005883	(detect$3 test$3) near3 detect$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:30
S16	6	(detect$3 test$3) near3 weak with key same (encrypt$3 cryptograph$2) not S2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:32
S17	17	(detect$3 test$3 identify identification reveal$3) with weak$3 with key same (encrypt$3 cryptograph$2) not S2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:34

EAST Search History

S18	16	(weak with semi adj weak) same (key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 21:42
S19	419	(726/6).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/06/12 22:02
S20	5	("5412717" | "5651068" | "5740248" | "5841869" | "5907620").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/06/12 22:02
S21	4	("6397330").URPN.	USPAT	OR	ON	2007/06/12 22:11
S22	1	("20040098619").PN.	US-PGPUB; USPAT	OR	OFF	2007/06/12 22:16
S23	1	("20050235342").PN.	US-PGPUB; USPAT	OR	OFF	2007/06/12 22:20
S24	281	test$3 with key with strength	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 22:21
S25	194	test$3 with key with strength same (encrypt$3 cryptograph$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 22:21
S26	49	test$3 with key with strength same (encrypt$3 cryptograph$2) not S6	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/12 22:21
S27	9	cipher adj strength near4 evaluation	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 18:17
S28	3	estimated adj key adj information	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 18:56

S29	3	estimated adj key same attack	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 18:20
S30	2	expected adj key same attack	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 18:20
S31	21	attack with estimate near5 key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 18:56
S32	34	attack with estimat$3 near5 key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 19:03
S33	393	(differential power) adj analysis with attack	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 19:05
S34	24	(differential power) adj analysis with attack and (weak$3 strength strong) near4 key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/13 19:13
S35	77	(380/1).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/06/13 19:13
S36	10	("5511123" | "5623548" | "5745577" | "5796837" | "5825886" | "6031911" | "6035042" | "6314186" | "6504929" | "6751319").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/06/13 19:14
S37	3	("6504929").URPN.	USPAT	OR	ON	2007/06/13 19:16
S38	5	("20020083134" | "5522022" | "6304790" | "6330527" | "6504929").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/06/13 19:18
S39	10	("5511123" | "5623548" | "5745577" | "5796837" | "5825886" | "6031911" | "6035042" | "6314186" | "6504929" | "6751319").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/06/13 19:18

EAST Search History

S40	0	("7051202").URPN.	USPAT	OR	ON	2007/06/13 19:19
S41	6	("6411715").URPN.	USPAT	OR	ON	2007/06/13 19:19

S42	9	("4200770" | "4218582" | "4376299" | "4405829" | "4691299" | "5272755" | "5351297" | "5606617" | "5768388").PN.	US-PGPUB;
			USPAT;
			USOCR
				OR	ON	2007/06/13 19:20